REMARKS

Fig. 5 of the drawings has been amended to correct a grammatical error. No new matter has been added.

The Examiner's allowance of claim 21 and the indication that claim 24 is drawn to allowable subject matter is noted with appreciation. The undersigned is of the opinion that the remaining claims are also entitled to allowance without further amendment, and presents the following remarks.

Claims 1, 5-7, 9, 12-14, 16 and 20 have been rejected as being anticipated by U.S. Patent 5,963,909 to Warren, claims 3 and 4 have been rejected as being obvious over a combination of Warren in view of U.S. Patent 6,643,402 to Okada, claims 8 and 15 have been rejected as being obvious over a combination of Warren in view of U.S. Patent 5,991,399 to Graunke, claim 10 has been rejected as being obvious over Warren in view of U.S. Patent 6,163,844 to Duncan, and claims 11 and 17-19 have been rejected as being obvious over a combination of Warren in view of Okada. Each of these rejections is traversed.

The invention is a system and method for controlling the access to and reproduction of encrypted digital information on a host system. As shown in the preferred embodiment in Fig. 2, after the compression and encryption steps the digital information is conveyed to the host system preferably with one of a plurality of decryption keys (see block 230), however as shown in Fig. 3, block 309, the host system may use alternate means to obtain decryption keys. Referring to Fig. 4, the decryption keys perform two functions. First, each key decrypts the digital information (block 407). Second, each key controls host system software, for example the media player application, to effect a different level and/or type of reproduction quality degradation on the media player (block 410). The level and type of reproduction quality degradation may be controlled by a time condition or a use condition, or alternatively, reproduction may be limited to only a portion of the digital information sought by the user. For example, quality may be degraded to a point where there is slight degradation (e.g., where coloration of the images are altered), or substantial or complete degradation may be effected (e.g., a scrambling effect or even a dark screen). To control reproduction quality in this

manner, the media player application preferably accesses a table of information which correlates each of the types of decryption keys with a certain reproduction quality. Ultimately, the user can purchase or otherwise obtain the decryption key referenced in block 310 of Fig. 3, which allows for continued viewing of the digital information without degradation.

In the Examiner's Response on page 2 of the office action, the Examiner stated that Warren teaches both the use of different types of decryption keys, and the key changing during different frames. However, this interpretation is incorrect in that Warren shows the us of tags, but the tags do not function to decrypt in the same or similar way to the claimed invention. The Warren reference describes a multi-media distribution system which includes a feature for either degrading or inhibiting a data signal that can be reproduced at a user's terminal based on the number of times the digital information is reproduced. Warren uses a standard master tag (SMT) and a standard copy tag (SCT) in conjunction with the multi-media signal, as shown in Figure 1. As is discussed in column 2, lines 36 et seq. and elsewhere in Warren, the SMT and SCT information may be spread spectrum signals which are preferably imperceptible when embedded in the data signal or they can be positioned in different layers (see, for example, Figures 9 and 10 of Warren). One embodiment discussed at column 11, lines 6 through 17 in Warren allows SCT information to overwrite SMT data every time the multi-media data is reproduced, thereby maintaining a copy generation number. The graceful degradation discussed in column 11 of Warren (referenced by the Examiner) discloses the addition of a predetermined amount of noise to outgoing data streams, the amount of which may be correlated with the copy generation number (see lines 33 through 42), and is independent of the encryption keys discussed in column 16 (for example, see lines 16 through 24). The Examiner has referenced column 16, lines 16-24, of Warren as suggesting the correlation of a first type of decryption key with a first type of reproduction quality, however this is an incorrect reading of Warren. The Warren reference does not disclose storing data on the host system which correlates a first type of decryption key with a first type of reproduction quality degradation performed based on at least one of the time

condition and the use condition, nor does Warren disclose a system of decryption keys to correlate with the type or level of degradation, if any, as contemplated by the invention. Thus, Warren is clearly not using a series of decryption keys, as contemplated by the present invention, to degrade or disable the ability to view an encrypted file, and to allow viewing the file without degradation. By contrast, the present invention will, for example, either degrade the signal which can be viewed or restrict the information that can be viewed based on the decryption key employed, and does not utilize embedded signal technology like that discussed in Warren. The present invention would offer enhanced security with less signal processing requirements when compared to Warren. These distinctions are highlighted in claim 1, as amended, and in claim 9, as originally filed and not amended.

In the Examiner's Response on page 3 of the office action, the Examiner stated that Warren teaches the use of different encryption keys, and that none of the Grauke, Duncan or Okada references were used to teach the utility of using different encryption keys. None of Graunke, Duncan or Okada make up for the deficiencies of Warren in that none of the references include a utility of using different decryption keys, disclose storing data on the host system which correlates a first type of decryption key with a first type of reproduction quality degradation performed based on at least one of the time condition and the use condition, nor disclose a system of decryption keys to correlate with the type or level of degradation, if any, as contemplated by the invention; therefore, no combination of Warren with Graunke, Duncan or Okada would make claims 1 or 9, or the respective dependent claims obvious.

The Graunke reference describes a secure distribution system, but utilizes only a single dynamically generated private key to allow access to a file by a particular user. The key in Graunke is not used to specify a degraded view of the transmitted file.

Duncan describes an access granting system with variable access rights; however, Duncan does not describe a series of decryption keys for allowing encyrpted files to viewed with varying integrity depending on the key used.

Okada describes an image compression device and system where the main advantage allows for the rapid and highly precise encoding of image data in a reduced amount of time (see column 8, lines 40-47). Column 19, lines 50-57, referenced by the Examiner, do not relate to using different encryption keys to control quality of a reproduced and transferred file; rather, this passage specifically relates to a system "whereby the degradation in quality of an image reproduced through the decompression of the compression image data can be prevented".

Okada describes an image compression device and system where the main advantage allows for the rapid and highly precise encoding of image data in a reduced amount of time (see column 8, lines 40-47). Column 19, lines 50-57, referenced by the Examiner, do not relate to using different decryption keys to control quality of a reproduced and transferred file; rather, this passage specifically relates to a system "whereby the degradation in quality of an image reproduced through the decompression of the compression image data can be prevented". Column 18, lines 6-12, 21-27, referenced by the Examiner, do not relate to a second type of decryption key as contemplated by the invention; rather, these passages relate to generating compression image data with reference to a particular quantization threshold value.

Claim 23 has been rejected as being anticipated by U.S. Patent 5,899,860 to Eller. This rejection is traversed.

Claim 23 is focused on one particular embodiment of the invention where a first decryption key at the host allows the application program reproducing the digital information to reproduce only a portion of the digital information. Claim 24 provides for a second decryption key at the host which allows for reproducing all of the digital information.

The system of Eller is quite distinct in that it distributes a file that is "partially" encrypted. This allows a client to hear part of the music for example. If he or she wants to purchase the music, he forwards payment and is furnished with a password that is specific to him or her. The password functions as a decryption key (see Abstract) which allows the user to hear all the music. Hence,

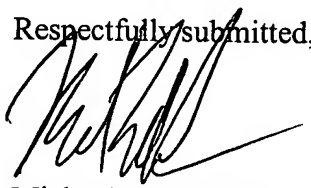
in claim 24. The passages cited by the Examiner support the undersigned's position. That is column 5, lines 65 et seq., discuss transfer of a file where "only the first page is not encrypted" (i.e., a decryption key is not used in Eller to provide a file where only some of the file can be seen; rather, the whole file is provided where a portion is encrypted—the key is provided after purchase). Further, in column 7, lines 51-65, of Eller do not describe having a "second" decryption key that lets one reproduce an entire file.

In view of the foregoing, it is respectfully requested that the application be reconsidered, that claims 1, 2-21, and 23-24 be allowed, and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

A provisional petition is hereby made for any extension of time necessary for the continued pendency during the life of this application. Please charge any fees for such provisional petition and any deficiencies in fees and credit any overpayment of fees to Attorney's Deposit Account No. 09-0457.

Respectfully submitted,



Michael E. Whitham
Reg. No. 32,635

Whitham, Curtis & Christofferson, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA 20190

Tel. (703) 787-9400
Fax. (703) 787-7557

Customer No.: 30743

ANNOTATED MARKED-UP DRAWINGS

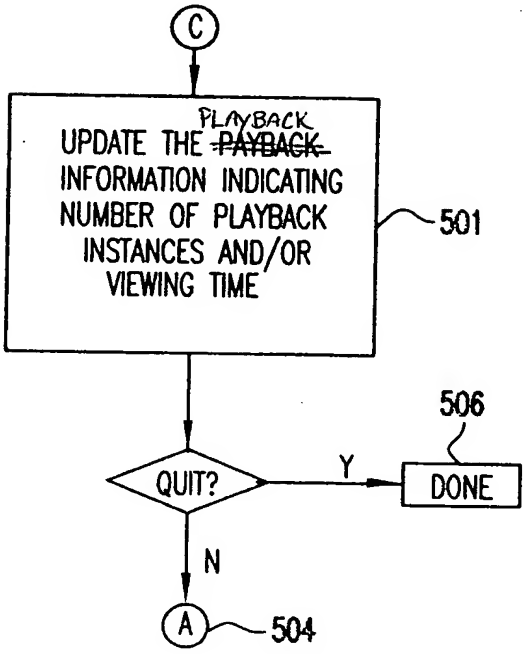


FIG.5